Esercizio epicode 20.11.2023

Nmap

Nmap è un tool open source per la scansione di reti, utilizza fondamentalmente due protocolli:

- TCP, per il threeway handshake
- ICMP, per il ping

Questo tool è molto versatile perché permette di effettuare vari tipi di scansioni da quelli più completi che però creano molta latenza (lenti), a quelli che creano meno rumore che però sono meno completi (veloci).

Scansione con Nmap

Eseguire una scansione con Nmap da macchina Kali Linux a Macchina Windows Xp, prima con il firewall non attivo e poi con il firewall attivo.

In quest'esercitazione abbiamo effettuato due scansioni con il comando -sV, che mi rivela le versioni delle porte aperte della macchina vittima.

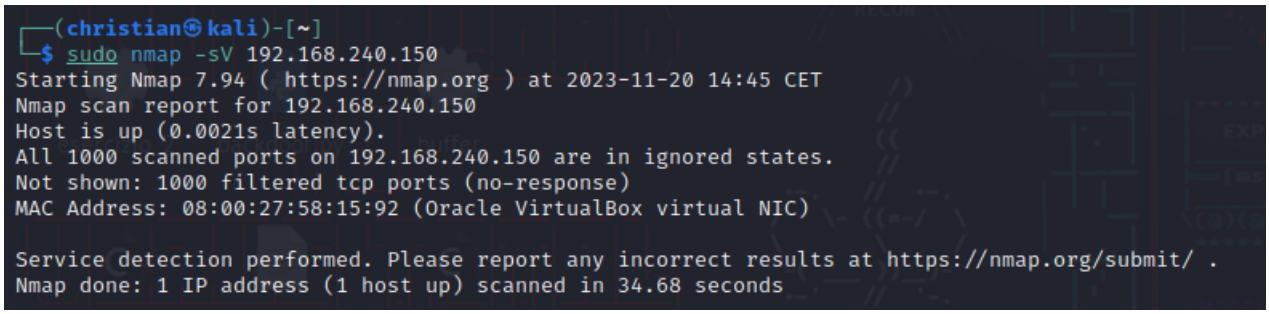
Con il firewall di windows disattivato, la scansione è andata a buon fine, ci rilevato tutte le porte aperte con le relative versioni.

```
┌──(christian㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150
[sudo] password for christian:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 14:38 CET
Nmap scan report for 192.168.240.150
Host is up (0.0022s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:58:15:92 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.75 seconds
```

Qua potremo già controllare le porte e le loro vulnerabilità per poterle sfruttare in un eventuale exploit con metaploit.

Invece eseguendo una scansione su Nmap con il firewall attivo, ci riporterà ad una serie di porte con “ignored states”.



Probabilmente il firewall blocca tutti i pacchetti in entrata del protocollo ICMP bloccando la scansione.

Per poter sviare a questo problema potremo creare una regola sul firewall per l’indirizzo IP della nostra macchina attaccante.